

REMARKS

Claims 1-9, 11-20, 24-27, 35-42 and 45 are pending in the present application. Claims 1, 2, 8, 11, 13-15, 17, 19 and 38-42 are amended above. Claims 21-23, 28-34, 43, 46 and 47 are cancelled above. New claims 48-87 are added above. Entry of the claim amendments and new claims is respectfully requested.

Claims 1-9, 11, 14, 18, 19, 35, 37-40 and 42 stand rejected under 35 U.S.C. 102(e) as being anticipated by Downs, *et al.* (U.S. Patent Number 6,226,618). Claims 24-27 and 45 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Mooney, *et al.* (U.S. Patent Number 6,351,813) in view of Bean, *et al.* (U.S. Patent Number 6,460,023). Claims 12, 13 and 15-17 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Downs, *et al.* in view of Horiike (U.S. Patent Number 6,744,905). Claim 20 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Downs, *et al.* in view of Ciacelli, *et al.* (U.S. Patent Number 6,236,727). Claim 36 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Downs, *et al.* in view of Mooney, *et al.* Claim 41 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Downs, *et al.* in view of Paulson, *et al.* (U.S. Patent Number 5,585,585). Reconsideration of the rejection and allowance of claims 1-20, 24-27, 35-42 and 45 are respectfully requested.

In the present invention as claimed in amended independent claim 1, a method for preventing unauthorized use of digital content data to be transferred from a first system to a second system includes locating an original archive of a digital content data at the first system, and determining transaction data of the second system that identifies the second system. The method further includes modifying the original archive using the transaction data of the second system that identifies the second system to generate a modified archive and transferring the modified archive from the first system to the second system. The method further includes receiving the transferred archive at the second system and recovering the digital content data of the original archive at the second system using the transaction data of the second system if the second system is a valid recipient.

Downs, *et al.* discloses that a Watermarking Tool is used to hide data in Content 113 that identifies the content and where it came from. This is referred to in Downs, *et al.* as a "Copyright Watermark" 529 (see Downs, *et al.*, column 22, lines 10-15 and the Table at columns 17 and 18, step 125). The Content 113 is packed into a Content SC(s) 630, and a Content Disbursement Tool sends the Content SC(s) 630 to a Content Housing 111 (see Downs, *et al.*, column 23, lines 29-45 and the Table at columns 17, 18 and 19, step 129). An End-User submits a purchase request to an Electronic Digital Content Store 103 for processing (see Downs, *et al.*, column 81, lines 10-16 and the Table at columns 17, 18 and 19, step 136). When the Electronic Digital Content Store 103 receives credit card authorization from the credit card clearing organization, a Transaction SC 640 is built by an SC Packer Tool (see Downs, *et al.*, column 81, lines 10-23, column 23, line 57 through column 24, lines 1-4 and the Table at columns 17, 18 and 19, step 138). The Transaction SC 640 includes all Offer SCs 641 for the Content 113 that the End-User has purchased, a Transaction ID 535 that can be tracked back to the Electronic Digital Content store 103, information that identifies the End-User, Transaction Data 642, compression levels and Usage Conditions 519 (see Downs, *et al.*, column 23, line 42 through column 24, line 4 and the Table at columns 17, 18 and 19, step 138). The Transaction SC 640 is transmitted to the End-User Device 109 (see Downs, *et al.*, column 23, line 57 through column 24, line 16 and the Table at columns 17, 18 and 19, step 139). Then, an Order SC 650 that contains, among other things, an Encrypted Symmetric Key 623 for the Content 113 including the Content Provider's 101 name, the encrypted Transaction Data 642 from the Transaction SC(s) 640 and End-User information, is sent to the Clearinghouse 105 for processing (see Downs, *et al.*, column 24, lines 5-16 and the Table at columns 17, 18 and 19, steps 141 and 142). The Clearinghouse 105 verifies that none of the data has been tampered with and validates the Usage Conditions purchased by the End-User (see Downs, *et al.*, column 24, lines 17-33 and the Table at columns 17, 18 and 19, step 143). Then, the Encrypted Symmetric Key 623 is decrypted using a private key of the Clearinghouse 105 (see Downs, *et al.*, column 24, lines 34-35, column 44, line 56 through column 45, line 6 and the Table at columns 17, 18 and 19, step 144). The Symmetric Key is then encrypted using a public key 661 of the End-User (see Downs, *et al.*, column 24, lines 34-40, column 44, line 56 through column 45, line 6 and the Table at

columns 17, 18 and 19, step 144). This new Encrypted Symmetric Key is then packaged into a License SC 660 by the SC Packer Tool (see Downs, *et al.*, column 24, lines 34-40, column 44, line 56 through column 45, line 6 and the Table at columns 17, 18 and 19, step 144). The License SC(s) 660 carries the Symmetric Key 623 and the Transaction Data 642, both encrypted using the public key 661 of the End-User device 109 (see Downs, *et al.*, column 24, lines 34-40, column 44, line 56 through column 45, line 6 and the Table at columns 17, 18 and 19, step 144). The License SC(s) 660 is transmitted to the End-User Device 109 (see Downs, *et al.*, column 24, lines 34-35 and the Table at columns 17, 18 and 19, step 145). After receiving the License LC(s) 660, the End-User Device 109 decrypts the Symmetric Key 623 and the Transaction Data 642 previously received from the Clearinghouse 105 and requests the Content SC(s) 630 from the Content Housing 111 (see Downs, *et al.*, column 24, lines 47-51 and the Table at columns 17, 18 and 19, step 146-147). Upon arrival of the Content SC(s) 630, the End-User Device 109 decrypts the Content 113 using the Symmetric Key 623 and passes the Content 113 and the Transaction Data to the other layers for license watermarking (see Downs, *et al.*, column 24, lines 51-57 and the Table at columns 17, 18 and 19, step 148). The End-User Device(s) 109 watermarks the copy of the Content 113, with the content purchaser's name and Transaction ID 535, and with other information such as date of license and Usage Conditions 517 (see Downs, *et al.*, FIG. 5, column 22, lines 10-24). This watermark is referred to in Downs, *et al.* as a "License Watermark" 527. Transaction Data 642 (see Downs, *et al.*, FIG. 6) provides user identity information to be included in the watermark of the Content 113 that is downloaded to the End-User(s) 109. The Transaction Data 642 includes the content purchaser's name, Transaction ID 535, date of license and Usage Conditions 517 (see Downs, *et al.*, column 76, lines 1-62). The Transaction ID 535 is downloaded to the End-User Device(s) 109 and used to watermark the Content 113 at the End-User Device(s) 109 (see Downs, *et al.*, column 7, lines 56-65, the Table at columns 17, 18 and 19, column 22, lines 9-24, column 23, line 1 through column 24, line 57, column 26, lines 24-29, column 28, lines 4-15, column 44, line 56 through column 45, line 6, column 45, lines 16-22, column 46, lines 8-24 and column 81, lines 43-61).

Downs, *et al.* discloses that the Content 113 is stored at the Content Housing 111. The End-User Device 109 sends an Order SC(s) to the Clearinghouse 105. The Clearinghouse 105 of Downs, *et al.* determines based on the Transaction Data whether the End-User Device 109 is a valid recipient and, if the End-User Device 109 is a valid recipient, sends the License SC(s) 660 to the End-User Device 109. The End-User Device 109 of Downs, *et al.* then requests the Content 113 and based on the validity of the License SC(s) 660, the Content 113 is transferred to the End-User Device 109. The Downs, *et al.* End-User Device 109 then watermarks the Content 113 with the Transaction Data 642. Downs, *et al.* states at column 76, lines 1-8, that the Transaction Data 642 is a structure of information provided by the transaction processing function of the Electronic Digital Content Store(s) 103 which is later used to correlate the Clearing house(s) 105 processing with the financial settlement transaction performed by the Electronic Digital Content Store(s) 103 and to provide user identity information to be included in the watermark of the Content 113 downloaded to the End-User Device 109. Therefore, in Downs, *et al.*, when the Content 113 is downloaded to the End-User Device 109, the Content 113 is watermarked with Transaction Data 642 that provides user identity information. At no point in the process of Downs, *et al.* is the Content 113 modified with Transaction Data 642 outside of the End-User Device 109. The Downs, *et al.* Content 113 is only modified with data of the End-User Device 109 at the End-User Device 109, and therefore, the modified Content 113 cannot be transferred to the End-User Device 109.

As stated in Amendment mailed on April 14, 2006, Downs, *et al.* fails to teach or suggest “modifying the original archive using the transaction data of the second system that identifies the second system to generate a modified archive” and “transferring the modified archive from the first system to the second system”, as claimed in independent claim 1. Instead, in Downs, *et al.*, the Content 113 is embedded with Transaction Data of the End-User Device(s) 109 after reception of the Content 113 at the End-User Device(s) 109. Therefore, in Downs, *et al.*, a “modified archive” is not transferred “from the first system to the second system” as claimed in claim 1. Instead, in Downs, *et al.*, the Content 113 is modified at the recipient system (End User Device(s) 109) following

transfer of the Content 113.

In addition, Downs, *et al.* fails to teach or suggest “receiving the transferred archive at the second system; and recovering the digital content data of the original archive at the second system using the transaction data of the second system if the second system is a valid recipient”, as claimed in independent claim 1. Instead, in Downs, *et al.*, the original Content 113 is received at the End-User Device(s) 109, decrypted using the Symmetric Key 623 including the Content Provider’s 101 name and then embedded with Transaction Data of the End-User Device(s) 109. The Symmetric key 623 of Downs, *et al.* used to decrypt the Content 113 is locally generated at the Content Provider 101 and in no way includes transaction data of the End-User Device(s) 109. The Transaction Data of the End-User Device(s) 109 of Downs, *et al.* is not used to recover the original Content 113, but rather is used to modify the Content 113 at the End-User Device(s) 109.

Accordingly reconsideration and removal of the rejection of claim 1 as being anticipated by Downs, *et al.*, are respectfully requested. With regard to dependent claims 2-9, 11, 14, 18, 19, 35, 37-40 and 42, it follows that these claims should inherit the allowability of the independent claim from which they depend.

With regard to the rejection of claims 12, 13 and 15-17 as being unpatentable over Downs, *et al.* and Horiike, Horiike is cited in the Office Action as teaching creating a map of the increased memory allocation. Horiike fails to teach or suggest “modifying the original archive using the transaction data of the second system that identifies the second system to generate a modified archive” and “transferring the modified archive from the first system to the second system”, as claimed in claim 1. In addition, Horiike fails to teach or suggest “receiving the transferred archive at the second system; and recovering the digital content data of the original archive at the second system using the transaction data of the second system if the second system is a valid recipient”, as claimed in independent claim 1.

Downs, *et al.* and Horiike, whether alone or in combination, fail to teach or

suggest “modifying the original archive using the transaction data of the second system that identifies the second system to generate a modified archive” and “transferring the modified archive from the first system to the second system” and “receiving the transferred archive at the second system and recovering the digital content data of the original archive at the second system using the transaction data of the second system if the second system is a valid recipient”, as claimed in independent claim 1.

Accordingly, it is submitted that the combination of Downs, *et al.* and Horiike fails to teach or suggest the invention as claimed in claims 12, 13 and 15-17. Reconsideration of the rejection of, and allowance of, claims 12, 13 and 15-17 are respectfully requested.

With regard to the rejection of claim 20 as being unpatentable over Downs, *et al.* and Ciacelli, *et al.*, Ciacelli, *et al.* is cited in the Office Action as teaching that the second system replaces the false data by the original data segments immediately prior to execution of the corresponding memory locations, and replaces the original data by the false data immediately following execution of the corresponding memory locations. Ciacelli, *et al.* fails to teach or suggest “modifying the original archive using the transaction data of the second system that identifies the second system to generate a modified archive” and “transferring the modified archive from the first system to the second system”, as claimed in independent claim 1. In addition, Ciacelli, *et al.* fails to teach or suggest “receiving the transferred archive at the second system and recovering the digital content data of the original archive at the second system using the transaction data of the second system if the second system is a valid recipient”, as claimed in independent claim 1.

Downs, *et al.* and Ciacelli, *et al.*, whether alone or in combination, fail to teach or suggest “modifying the original archive using the transaction data of the second system that identifies the second system to generate a modified archive” and “transferring the modified archive from the first system to the second system” and “receiving the transferred archive at the second system and recovering the digital content data of the

original archive at the second system using the transaction data of the second system if the second system is a valid recipient”, as claimed in independent claim 1.

Accordingly, it is submitted that the combination of Downs, *et al.* and Ciacelli, *et al.* fails to teach or suggest the invention as claimed in claim 20. Reconsideration of the rejection of, and allowance of, claim 20 are respectfully requested.

With regard to the rejection of claim 36 as being unpatentable over Downs, *et al.* and Mooney, *et al.*, Mooney, *et al.* is cited in the Office Action as teaching that a unique identifying value is used to create a system unique encryption key. Mooney, *et al.* fails to teach or suggest “modifying the original archive using the transaction data of the second system that identifies the second system to generate a modified archive” and “transferring the modified archive from the first system to the second system”, as claimed in independent claim 1. In addition, Mooney, *et al.* fails to teach or suggest “receiving the transferred archive at the second system and recovering the digital content data of the original archive at the second system using the transaction data of the second system if the second system is a valid recipient”, as claimed in independent claim 1.

Downs, *et al.* and Mooney, *et al.*, whether alone or in combination, fail to teach or suggest “modifying the original archive using the transaction data of the second system that identifies the second system to generate a modified archive” and “transferring the modified archive from the first system to the second system” and “receiving the transferred archive at the second system and recovering the digital content data of the original archive at the second system using the transaction data of the second system if the second system is a valid recipient”, as claimed in independent claim 1.

Accordingly, it is submitted that the combination of Downs, *et al.* and Mooney, *et al.* fails to teach or suggest the invention as claimed in claim 36. Reconsideration of the rejection of, and allowance of, claim 36 are respectfully requested.

With regard to the rejection of claim 41 as being unpatentable over Downs, *et al.*

and Paulson, *et al.*, Paulson, *et al.* is cited in the Office Action as teaching that if it is determined that the second system is an invalid recipient of the archive, further modifying the archive into an archive that would cause an exit, and error condition, or communication to another system entity which begins a cascading exit process, in the second system, and transferring the further modified archive to the second system. Paulson, *et al.* fails to teach or suggest “modifying the original archive using the transaction data of the second system that identifies the second system to generate a modified archive” and “transferring the modified archive from the first system to the second system”, as claimed in independent claim 1. In addition, Paulson, *et al.* fails to teach or suggest “receiving the transferred archive at the second system and recovering the digital content data of the original archive at the second system using the transaction data of the second system if the second system is a valid recipient”, as claimed in independent claim 1.

Downs, *et al.* and Paulson, *et al.*, whether alone or in combination, fail to teach or suggest “modifying the original archive using the transaction data of the second system that identifies the second system to generate a modified archive” and “transferring the modified archive from the first system to the second system” and “receiving the transferred archive at the second system and recovering the digital content data of the original archive at the second system using the transaction data of the second system if the second system is a valid recipient”, as claimed in independent claim 1.

Accordingly, it is submitted that the combination of Downs, *et al.* and Paulson, *et al.* fails to teach or suggest the invention as claimed in claim 41. Reconsideration of the rejection of, and allowance of, claim 41 are respectfully requested.

Hollar (U.S. Patent Number 7,124,114) is cited in an Information Disclosure Statement filed contemporaneously herewith. Hollar discloses a method and system in which a client requests digital content from a distribution server. The distribution server, in turn, requests that the client provide identification information. If the client complies and provides the requested identification, then the distribution server determines whether

a record of the client identification appears in a piracy history database. Assuming the distribution server determines that a copy is to be sent to the client, a copy is distributed to the recipient that includes identifications of the digital content and recipient embedded into it as an identifier that remains with the digital content. A detection server samples content from various distribution channels and updates the piracy database of the distribution server accordingly. With regard to amended independent claim 1, Hollar, like Downs, *et al.*, fails to teach or suggest "receiving the transferred archive at the second system and recovering the digital content data of the original archive at the second system using the transaction data of the second system if the second system is a valid recipient". Instead, in Hollar, the original content is not recovered at the recipient and the identifications of the recipient embedded into the content are not used to recover the original content, but rather, instead remain with the original content as an identifier for tracking future piracy.

With regard to the rejection of claims 24-27 and 45 based on the combination of Mooney, *et al.* and Bean, *et al.*, the present Office Action makes no specific reference to the substance of the Applicant's remarks submitted in the Amendment dated April 14, 2006, other than to combine, in the present Office Action, the teachings of Mooney, *et al.* and Bean, *et al.* in formulating the current rejection. The Applicant specifically addresses the rejection of claim 44 in view of the combined teachings of Mooney, *et al.* and Bean, *et al.* in the Amendment dated April 24, 2006, in connection with the incorporation of the limitation of then dependent claim 44 into independent claim 24. Since these arguments still apply, and since no specific answer to the substance of the Applicant's argument, or no new grounds for rejection, have been presented in the current Office Action, the arguments are primarily repeated below, in connection with the current rejection.

In the present invention as claimed in independent claim 24, a method for preventing unauthorized use of digital content data hosted on a system includes, determining whether an unauthorized use of digital content data is in progress, and in the case where an unauthorized use is determined, initiating a defense action by disabling

only an input device in association with the unauthorized use. The input device is only disabled in an unauthorized interface window when the target focus for the input device is an unauthorized application associated with the unauthorized interface window.

It is stated in the Office Action at page 10, paragraph 3 that Mooney, *et al.* does not disclose expressly that the input device is only disabled in an unauthorized interface window when the target focus for the input device is an unauthorized application associated with the unauthorized interface window.

Therefore Mooney, *et al.* fails to teach or suggest determining whether an unauthorized use of digital content data is in progress, and “in the case where an unauthorized use is determined, initiating a defense action by disabling only an input device in association with the unauthorized use, wherein the input device is only disabled in an unauthorized interface window when the target focus for the input device is an unauthorized application associated with the unauthorized interface window”, as claimed in claim 24.

As stated in the Amendment mailed on April 14, 2006, Bean, *et al.* discloses a software authorization method which permits a developer to provide licensed software content files to a customer. In Bean, *et al.*, authorized content files are downloaded to users of a customer's site. Only content files embedded in the authorized Web pages or domain names may be displayed or executed on the users' computer. If the content is not authorized, the user views a watermark that indicates that a rich media asset is not properly licensed and that obstructs the display of the rich media asset or causes the display of an error message. In FIG. 4 of Bean, *et al.*, each of windows 70, 74 and 76 are counted as a single authorized use of the content so that there are three authorized uses. In Bean, *et al.*, the output of the content is obstructed or an error message is displayed during an unauthorized use.

Bean, *et al.* fails to teach or suggest determining whether an unauthorized use of

digital content data is in progress, and “in the case where an unauthorized use is determined, initiating a defense action by disabling only an input device in association with the unauthorized use, wherein the input device is only disabled in an unauthorized interface window when the target focus for the input device is an unauthorized application associated with the unauthorized interface window”, as claimed in claim 24. Instead, in Bean, *et al.*, the output of the content is obstructed or an error message is displayed during an unauthorized use. Therefore, an output device is disabled in an unauthorized window during an unauthorized use in Bean, *et al.*, rather than an “input device” as claimed in claim 24. Bean, *et al.* in no way teaches or suggests that an “input device” is disabled.

Mooney, *et al.* and Bean, *et al.*, whether alone or in combination, fail to teach or suggest determining whether an unauthorized use of digital content data is in progress, and “in the case where an unauthorized use is determined, initiating a defense action by disabling only an input device in association with the unauthorized use, wherein the input device is only disabled in an unauthorized interface window when the target focus for the input device is an unauthorized application associated with the unauthorized interface window”, as claimed in claim 24.

Accordingly, it is submitted that the combination of Mooney, *et al.* and Bean, *et al.* fails to teach or suggest the invention as claimed in claims 24, 25, 26 and 45. Reconsideration of the rejection of, and allowance of, claims 24, 25, 26 and 45 are respectfully requested.

New claims 54-87 are added above. New independent claim 54 is directed to a method of preventing unauthorized use of digital content data to be transferred from a first system to a second system that includes “determining transaction data” of a “second system that identifies the second system by executing an analysis tool to examine components of the second system and to generate a unique identifying value, the unique identifying value identifying the second system and being based on selected properties of

the examined components, the transaction data comprising the unique identifying value". While the Office Action states at page 6, second paragraph, referring to dependent claim 7, that Downs teaches "determining transaction data of the second system comprises downloading an analysis tool to the second system, and running the analysis tool to examine the second system and to generate a unique identification value that identifies the second system as the transaction data," neither of the End-User Player Application 195 and the Watermarking Tool of Downs, *et al.* examine the End-User Device(s) 109 and generate a unique identification value that identifies the second system as the transaction data. Accordingly, allowance of new claims 54-87 is respectfully requested.

Similarly, there is no teaching or suggestion in Hollar (U.S. Patent Number 7,124,114), described above, and cited in an Information Disclosure Statement filed contemporaneously herewith, of a method of preventing unauthorized use of digital content data to be transferred from a first system to a second system that includes "determining transaction data" of a "second system that identifies the second system by executing an analysis tool to examine components of the second system and to generate a unique identifying value, the unique identifying value identifying the second system and being based on selected properties of the examined components, the transaction data comprising the unique identifying value", as claimed in new independent claim 54. In Hollar, there is no mention of such an analysis tool or its operation.

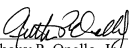
Closing Remarks

It is submitted that all claims are in condition for allowance, and such allowance is respectfully requested. If prosecution of the application can be expedited by a telephone conference, the Examiner is invited to call the undersigned at the number given below.

Respectfully submitted,

Date: November 10, 2006
Mills & Onello, LLP
Eleven Beacon Street, Suite 605
Boston, MA 02108
Telephone: (617) 994-4900, Ext. 4902
Facsimile: (617) 742-7774

J:\ECD\0003\AmendC-elect\AmendC-elect.wpd


Anthony P. Onello, Jr.
Registration Number 38,572
Attorney for Applicant